IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: :

    Christopher van Es   :

Application. No.: TBD   :   Group Art Unit: TBD

                                      :

Filed: September 30, 2003   :   Examiner: TBD

Title: AUTHENTICATION SYSTEM

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

     A certified copy of corresponding Great Britain Application No. 0311097.0, filed May 14, 2003 is attached. It is requested that the right of priority provided by 35 U.S.C. 119 be extended by the U.S. Patent and Trademark Office.

                                                Respectfully submitted,

Date: September 30, 2003

Michael A. Schwartz, Reg. No. 40,161
Swidler Berlin Shereff Friedman, LLP
3000 K Street, NW, Suite 300
Washington, DC 20007-5116
Telephone: (202) 424-7500
Facsimile: (202) 295-8478

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation and Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein together with the Statement of inventorship and of right to grant of a Patent (Form 7/77), which was subsequently filed.
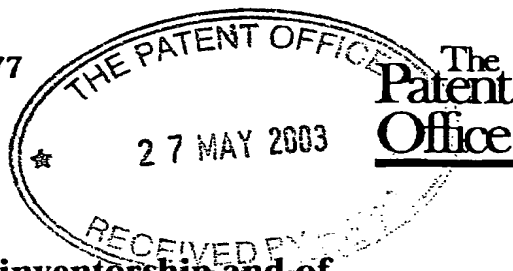
In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.
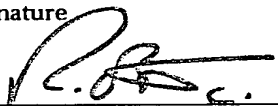
Signed

Dated   9 July 2003

Patents Form 7/77

Patents 1977
(Rule 15)

THE PATENT OFFICE
27 MAY 2003
RECEIVED BY

The
Patent
Office

7/77

28MAY03 13290-1 07041
R 7/77 0.0 03110 .0

Statement of inventorship and of
right to grant of a patent

1.	Your reference	RSJ07777GB
2.	Patent application number *(if you know it)*	0311097.0
3.	Full name of the or of each applicant	Oracle International Corporation
4.	Title of the invention	AUTHENTICATION SYSTEM
5.	State how the applicant *(s)* derived the right from the inventor *(s)* to be granted a patent	By employment.
6.	How many, if any, additional Patents Forms 7/77 are attached to this form? *(see note (c))*	

7. For the applicant
Gill Jennings & Every

I/We believe that the person *(s)* named over the page *(and on any extra copies of this form)* is/are the inventor *(s)* of the invention which the above patent application relates to.

Signature

Date
27 May 2003

8.	Name and daytime telephone number of person to contact in the United Kingdom	SKONE JAMES, Robert Edmund 020 7377 1377

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there are more than three inventors, please write the names and addresses of the other inventors on the back of another Patents Form 7/77 and attach it to this form.*

d) *When an application does not declare any priority, or declares priority from an earlier UK application, you must provide enough copies of this form so that the Patent Office can send one to each inventor who is not an applicant.*

e) *Once you have filled in the form you must remember to sign and date it.*

Patents Form 7/77

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

Christopher <u>van Es</u>
74 Church Road
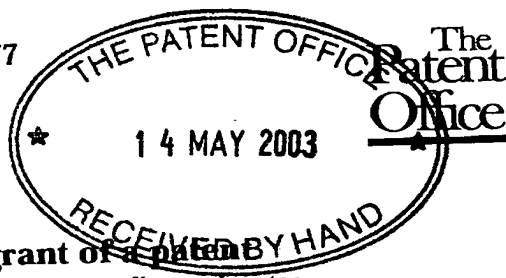Woodley
Reading
RG5 4QB
Great Britain

Patents ADP number *(if you know it):* 864160 7001

Patents ADP number *(if you know it):*

Patents ADP number *(if you know it):*

Reminder

Have you signed the form?

Patents Form 1/77

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
14 MAY 2003
RECEIVED BY HAND

The Patent Office

15MAY03 EC07305-6 002B90
P01/7700 0.00-0311097.0

1 7 7

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

14 MAY 2003

1.	Your reference	RSJ07777GB

2.	Patent application number *(The Patent Office will fill in this part)*	**0311097.0**

3.	Full name, address and postcode of the or of each applicant *(underline all surnames)*	Oracle International Corporation 500 Oracle Parkway M/S 5op7, Redwood Shores California 94065 USA
	Patents ADP number *(if you know it)*	
	If the applicant is a corporate body, give the country/state of its incorporation	Delaware, USA 837301001

4.	Title of the invention	Authentication System

5.	Name of your agent *(if you have one)*	Gill Jennings & Every
	"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	Broadgate House 7 Eldon Street London EC2M 7LH
	Patents ADP number *(if you know it)*	745002

	Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*
6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number			

	Number of earlier application	Date of filing *(day / month / year)*
7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application		

8.	Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*	YES
	a) any applicant named in part 3 is not an inventor, or	
	b) there is an inventor who is not named as an applicant, or	
	c) any named applicant is a corporate body.	
	See note (d))*	

Patents Form 1/77

9. Enter the number of sheets for any of the
   following items you are filing with this form.
   Do not count copies of the same document

Continuation sheets of this form

Description	6
Claim(s)	3	C F
Abstract	-
Drawing(s)	2 + 2

10. If you are also filing any of the following,
    state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	I
Request for substantive examination *(Patents Form 10/77)*	I
Any other documents *(please specify)*	NO

11. For the applicant
    Gill Jennings & Every

I/We request the grant of a patent on the basis of this application.

Signature

Date 14 May 2003

12. Name and daytime telephone number of
    person to contact in the United Kingdom

R.E. Skone James

020 7377 1377

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

AUTHENTICATION SYSTEM

This invention relates to authentication of a user and, in particular, to a biometric contact sensor and its method of operation for achieving this purpose.

Fingerprint sensors are well known biometric contact sensors that are used as a means for confirming the identity of an individual in order to grant access to a secure environment or for logging on to a computer system. Three types of fingerprint sensors are typically used. These are capacitive, optical and thermal sensors. A capacitive sensor comprises an array of miniature capacitors in which the surface of the skin of a fingertip placed on the sensor acts as a capacitive pole. As such the capacitance of each miniature capacitor depends on whether a ridge or furrow of the fingerprint forms the capacitive pole of that particular miniature capacitor. Optical sensors function by illuminating the fingertip and capturing an image using a CCD or CMOS camera. The third type of sensor, the thermal sensor, measures the small temperature difference between the ridges and furrows of the fingertip.

However, a problem exists regarding the security of such fingerprint sensors since, under certain circumstances, it is possible to gain access to the secure environment protected by a fingerprint sensor using the latent image of a fingerprint left on the device by the preceding user. It has been found that it is possible to use a latent image to gain access to the secure environment protected by the fingerprint sensor by carefully placing a plastic bag filled with water on to the sensor's surface or even merely by breathing on the sensor's surface.

A proposed solution is to provide a cover that slides over the sensor when it is not being used. The underside of the cover has a sponge loaded with a suitable solvent to remove the latent image. However, this increases the complexity of the sensor, requires maintenance and is

straightforward to defeat. Clearly, there exists a need for a fingerprint sensor that combines the ease of use of a conventional sensor whilst offering higher security.

In accordance with one aspect of the present invention, there is provided a method of authenticating the identity of a user, the method comprising:

a. placing, in sequence, each of a plurality of parts of the user's body on a biometric contact sensor at a sensing position;

b. obtaining from the sensor a data set of biometric contact characteristics for each of the plurality of body parts;

c. comparing each data set with authentic versions stored in a database; and,

d. issuing an authentication signal if the data sets satisfactorily match the corresponding authentic versions.

Hence, the invention utilises the fact that the latent image of a body part can be obscured by placing another body part on top of it. The invention thus prevents the use of a latent image left upon the biometric contact sensor by the preceding user in order to gain access to the secure environment that it protects.

In a preferred embodiment, the body parts are the user's fingertips and the biometric contact sensor is a fingerprint sensor.

Typically, each part of the user's body must be placed on the biometric contact sensor within a predetermined time period before the authentication signal will be issued.

In a preferred embodiment, before issuing the authentication signal, it is confirmed that the sequence of data sets was obtained in a predetermined order.

Any suitable algorithm may be used to compare the data sets with the authentic versions. However, either a minutiae based algorithm or a correlation based algorithm will typically be used.

In accordance with a second aspect of the present invention, there is provided apparatus for authenticating a user, the apparatus comprising a fingerprint sensor capable of sensing only one fingerprint at a time, and a

5 processor and a database adapted to perform a method according to the first aspect of the present invention.

Any fingerprint sensor may be used with the apparatus but typically, the fingerprint sensor will be a capacitive sensor, an optical sensor or a thermal sensor.

10 The apparatus may further comprise a data input device, for example, to enter a user name or number. The data input device may be any suitable data input device but typically, it will be a keypad or smart card reader.

In accordance with a third aspect of the present

15 invention, there is provided a method of authenticating the identity of a user, the method comprising:

a. obtaining a sequence of data sets of biometric characteristics of the user, each data set relating to one of a plurality of parts of the user's body;

20 b. comparing each data set with authentic versions stored in a database;

c. monitoring the order in which the sequence of data sets was obtained; and,

d. issuing an authentication signal if the data sets

25 satisfactorily match the corresponding authentic versions and the sequence of data sets was obtained in a predetermined order.

Biometric characteristics may be obtained for any part of the user's body. However, typically, the plurality of

30 parts of the user's body will include the user's fingertips, retinas or face or a combination of any of these.

Various types of sensors may be used to perform this aspect of the invention. For example, a retina scanner may

35 be used to obtain biometric characteristics of a user's retina and a fingerprint sensor may be used to obtain biometric characteristics of a user's fingertips.

Such sensors may be capable of obtaining more than one data set of biometric characteristics at a time. For example, the biometric characteristics of both retinas or of several fingertips may be obtained simultaneously.

5   An embodiment of the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 shows a schematic of apparatus according to the invention; and,

Figure 2 shows a device incorporating the apparatus of
10   Figure 1.

Figure 1 shows a fingerprint sensor 1 attached to a processor 2 to which is also connected a database 3 and a data input device 4. The fingerprint sensor 1 has a sensor array (not shown) that is sized such that it can only sense
15   one fingerprint at a time. A device 10 incorporating the fingerprint sensor 1 and data input device 4, in the form of a keypad, is shown in Figure 2.

The database 3 stores authentic versions of the fingerprint data sets of users authorised to access the
20   system protected by the fingerprint sensor 1. The fingerprint sensor 1 may be of any known type including capacitive, optical and thermal variants. It may be used, for example, to control access to a computer system or to unlock the door to a secure room.

25   The data input device 4 may be any of a variety of such devices, for example, a keypad or touchscreen. In this example, the data input device 4 is a keypad. A user wishing to access the secure environment must firstly enter a user name or number into the data input device 4. This
30   identifies to the processor 2 who the user claims to be. In order to authenticate his identity, the user must then place each of his required fingertips on the fingerprint sensor 1 in sequence and in the correct order. For example, the system may be configured such that in order
35   for a particular user to gain access, that user must place the index, ring and middle fingers of his right hand

followed by the thumb of his left hand on the fingerprint sensor 1 in that order.

The fingerprint sensor 1 obtains a fingerprint data set for each fingertip placed upon it. This fingerprint data set is passed to the processor 2 which compares it with the authentic versions of the fingerprint data sets of authorised users already recorded that are stored in database 3. The processor 2 performs this comparison using any one of many suitable algorithms to confirm that a satisfactory match exists between the fingerprint data set obtained by the fingerprint sensor 1 and the corresponding authentic version stored in data base 3, that is to say that there is a sufficient correlation between the two data sets that the identity of the user can be assumed to be authentic.

Typically, either a minutiae-based algorithm or a correlation-based algorithm will be used. The minutiae-based algorithms isolate the minutiae points of a fingerprint (interruptions to the lines upon the fingertips) and determine their relative placement on the finger whilst the correlation-based algorithm directly compares the two fingerprint data sets to determine whether a sufficiently high correlation exists between them.

Provided that the results of this comparison by processor 2 confirm that the fingertips placed on the fingerprint sensor do indeed belong to the user then the processor 2 proceeds to confirm that the fingertips of the user were placed on the fingerprint sensor 1 in the required order. If this criterion is met, then the processor 2 will issue an authentication signal on output 5 indicating that the identity of the user is authentic.

In a variation of this embodiment, the apparatus can be provided with a display (not shown) and the processor 2 is adapted to cause the display to indicate which fingertip the user must place on the fingerprint sensor 1 next. This allows the required order to be changed each time the user uses the system or at other, for example, random intervals.

The output 5 may be in any one of a variety of known formats. For example, it may be a USB output for connection to a personal computer or other electronic device or alternatively, it may be a wireless medium such as a Bluetooth connection.

A further requirement that may be imposed is that each fingertip of the user must be placed on the fingerprint sensor within a predetermined time period. This will allow the processor 2 to revert to the beginning of the authentication process if a user only partially completes a previous authentication.

Aside from using second and subsequent placement of fingertips on the fingerprint sensor 1 to obscure the latent image of a first fingerprint, the invention, as described with respect to this embodiment, provides an additional advantage. That is, by having to know which fingers must be placed on the fingerprint sensor 1 and in which order, a certain level of "password" protection is also afforded by the system.

A further level of security can be provided if, instead of data input device 4 being a key pad, a smart card reader is used into which the user inserts a smart card unique to him instead of entering a user name or number.

Another possibility is to remove data input device 4 altogether and for the user merely to place the correct fingertips on the fingerprint sensor 1 in the correct order. In this instance, the processor 2 must infer the identity of the user from the fingerprint data sets stored in database 3.

CLAIMS

1. A method of authenticating the identity of a user, the method comprising:

    a. placing, in sequence, each of a plurality of parts of the user's body on a biometric contact sensor at a sensing position;

    b. obtaining from the sensor a data set of biometric contact characteristics for each of the plurality of body parts;

    c. comparing each data set with authentic versions stored in a database; and,

    d. issuing an authentication signal if the data sets satisfactorily match the corresponding authentic versions.

2. A method according to claim 1, wherein the body parts are the user's fingertips and the biometric contact sensor is a fingerprint sensor.

3. A method according to either of the preceding claims, wherein each part of the user's body must be placed on the biometric contact sensor within a predetermined time period before the authentication signal will be issued.

4. A method according to any of the preceding claims, further comprising the step of confirming that the sequence of data sets was obtained in a predetermined order before issuing the authentication signal.

5. A method according to any of the preceding claims, wherein the data sets are compared with the authentic versions using a minutiae based algorithm.

6. A method according to any of the preceding claims, wherein the data sets are compared with the authentic versions using a correlation based algorithm.

7. Apparatus for authenticating a user, the apparatus comprising a fingerprint sensor capable of sensing only one fingerprint at a time, and a processor and a database adapted to perform a method according to any of the preceding claims.

8.   Apparatus according to claim 7, wherein the fingerprint sensor is a capacitive sensor.

9.   Apparatus according to claim 7, wherein the fingerprint sensor is an optical sensor.

5   10.   Apparatus according to claim 7, wherein the fingerprint sensor is a thermal sensor.

11.   Apparatus according to any of claim 7 to 10, further comprising a data input device.

12.   Apparatus according to claim 11, wherein the data
10   input device is a keypad.

13.   Apparatus according to claim 11, wherein the data input device is a smart card reader.

14.   A method of authenticating the identity of a user, the method comprising:

15   a.   obtaining a sequence of data sets of biometric characteristics of the user, each data set relating to one of a plurality of parts of the user's body;

       b.   comparing each data set with authentic versions
20   stored in a database;

       c.   monitoring the order in which the sequence of data sets was obtained; and,

       d.   issuing an authentication signal if the data sets satisfactorily match the corresponding
25   authentic versions and the sequence of data sets was obtained in a predetermined order.

15.   A method according to claim 14, wherein at least one of the plurality of parts of the user's body is a fingertip.

30   16.   A method according to claim 14 or claim 15, wherein at least one of the plurality of parts of the user's body is a retina.

17.   A method according to any of claims 14 to 16, wherein at least one of the plurality of parts of the user's body
35   is the user's face.

18.   A method substantially as hereinbefore described with reference to the accompanying drawings.

19.   Apparatus substantially as hereinbefore described with reference to the accompanying drawings.

ABSTRACT

<u>AUTHENTICATION SYSTEM</u>

5   A method of authenticating the identity of a user is described. Each of a plurality of parts of the user's body are placed, in sequence, on a biometric contact sensor at a sensing position.

         A data set of biometric contact characteristics for
10   each of the plurality of body parts is obtained from the sensor.

         Each data set is compared with authentic versions stored in a database and an authentication signal is issued if the data sets satisfactorily match the corresponding
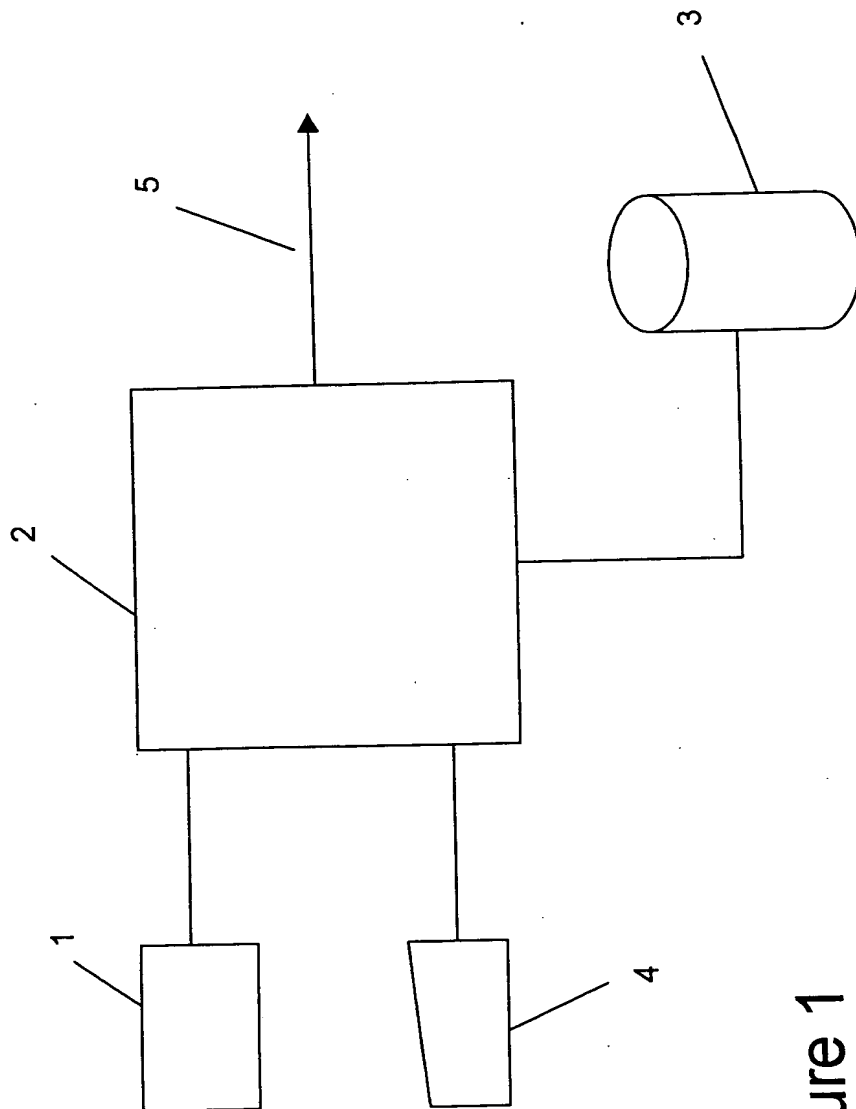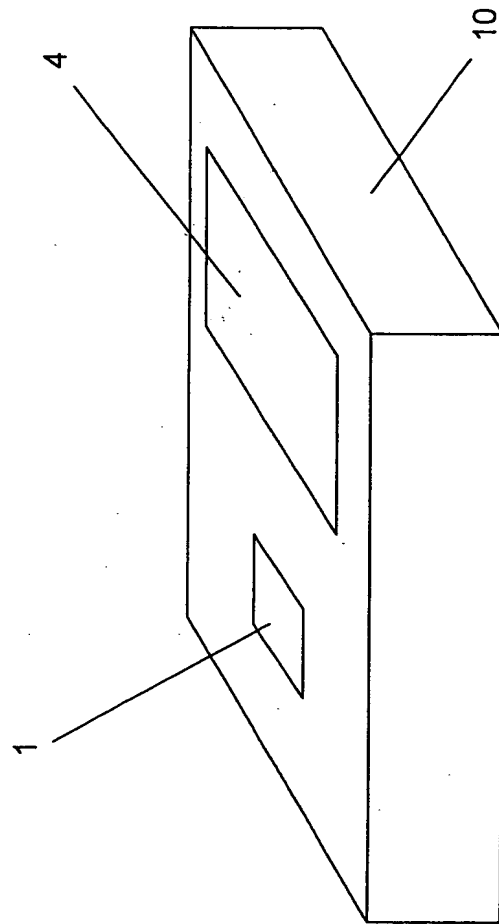15   authentic versions.

[Figure 1]

Figure 1

Figure 2